

AU/ACSC/36-2114/2004-05

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

THE DEATH OF INFORMATION OPERATIONS:
MAKING THE CASE FOR NON-KINETIC OPERATIONS

by

Kelly G. Robinson, Major, U.S. Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Instructor: Kirk A. Kimmett, Major, U.S. Air Force

Maxwell Air Force Base, Alabama

April 2005

Distribution A: Approved for Public Release; Distribution is Unlimited
--

Report Documentation Page		Form Approved OMB No. 0704-0188
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.		
1. REPORT DATE APR 2005	2. REPORT TYPE	3. DATES COVERED 00-00-2005 to 00-00-2005
4. TITLE AND SUBTITLE THE DEATH OF INFORMATION OPERATIONS: MAKING THE CASE FOR NON-KINETIC OPERATIONS		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER	
	5e. TASK NUMBER	
	5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air University Press (AUL/LP),131 W Shumacher Avenue,Maxwell AFB,AL,36112-6615		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited		
13. SUPPLEMENTARY NOTES		
14. ABSTRACT <p>Across the Air Force, Airmen agree that Information Operations (IO) is a topic worthy of our attention, but few Airmen can agree on exactly what IO is. The primary source of this confusion traces back to the very label we are using. The word information in its name implies a direct and exclusive relationship between IO and Information Superiority as well as the Information Domain. Another contributing factor is the persistent confusion between influence capabilities, provided by IO, and influence effects, the essence of all warfare. In the end, reliance on information as the common denominator for this set of capabilities eventually led to IO tribalism within the Air Force and an inefficient "everything is IO" mindset. If Air Force IO is going to provide relevant and useful engagement options to commanders, it must bring specific capabilities to the fight not already clearly defined in our air warfare, space operations, or mobility doctrine. The Air Force made significant progress by streamlining its version of IO in January 2005, but still did not clearly define a replacement for information as the entrance qualifier for IO doctrine. Without a common "glue" to bind these capabilities, IO is simply a conglomeration of unrelated and otherwise orphaned mission areas. This research paper examines IO concept development over the last decade and investigates some of the problems resulting from recent Air Force IO terminology and doctrine. Based on a vision for the seamless integration of kinetic and non-kinetic capabilities, this paper proposes discarding the misnomer IO in favor of a new term, "Non-Kinetic Operations". More than just a name change, this new label represents the glue that binds Electronic Warfare, Influence Operations, and Network Warfare Operations. By adopting Non-Kinetic Operations as the next generation of Air Force IO, we can finally focus on "Integrated Operations", the only "IO" that really matters in joint effects based operations.</p>		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 37	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the United States Government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States Government.

Table of Contents

	Page
<i>DISCLAIMER</i>	i
<i>ACKNOWLEDGEMENTS</i>	iii
<i>ABSTRACT</i>	iv
INTRODUCTION	1
DEFINING INFORMATION OPERATIONS	3
Complicated by Tribal Perspectives	3
The Information Domain	5
Struggling with Terminology	6
AIR FORCE INFORMATION OPERATIONS 1994-2004	9
TEARING DOWN IO STOVEPIPES	14
The “Less is More” Approach to Information Operations	15
Capabilities and Effects	17
The Essence of Warfare	18
RECOMMENDING A NEW VISION FOR USAF INFORMATION OPERATIONS	20
Making the Case for Non-Kinetic Operations	22
Information Superiority	25
CONCLUSION	27
<i>BIBLIOGRAPHY</i>	30

List of Figures

	Page
FIGURE 1: Air Force IO Construct (2002)	11
FIGURE 2: Everything is IO (2002)	12
FIGURE 3: Non-Kinetic Operations (2005)	24
FIGURE 4: The Family of Air Force Doctrine	26

Acknowledgements

This paper is the result of mentoring and invaluable assistance from a number of people. The first thanks must go to General (ret) Hal M. Hornburg, former Commander of Air Combat Command. In the fall of 2002, he tasked his Commander's Action Group (CAG) to help him integrate conflicting community perspectives into a single vision for Air Force Information Operations (IO). For two years, it was my privilege to assist the General in articulating his IO vision by way of several CORONA briefings, COMACC Sight Pictures, and participation in the rewrites of the Air Force IO CONOPS (2004) and AFDD 2-5: *Information Operations* (2005). General Hornburg's vision, leadership, and initiative made this transformation of Air Force IO possible. I cannot express how much I learned as a member the ACC CAG.

I would also thank Brig Gen (ret) Ben Robinson for encouraging me to challenge existing dogma and to always look for the big picture. He clearly demonstrated the power of leadership vision as he led the 552d Air Control Wing through the terrorist attacks on 11 September 2001. I will always be grateful for his mentorship and do my very best to pay it forward.

Finally, I must thank the many outstanding officers I served with on the ACC staff. The seventeen officers I worked with in two years on the ACC CAG all exemplified the highest standards of integrity, professionalism, work ethic, and continual learning. In particular, Lt Cols Tim Gibson, Alex DeFazio, and Major Mike Dombrowski continuously challenged my IO ideas, offered their own, and kept me from drifting astray. I am also extremely appreciative for the IO education I received from the real subject matter experts in ACC/DOZ and ACC/SC. All of these officers deserve full credit for any good ideas found on the following pages, while I take full responsibility for any bad ideas you may find.

Abstract

Across the Air Force, Airmen agree that Information Operations (IO) is a topic worthy of our attention, but few Airmen can agree on exactly what IO is. The primary source of this confusion traces back to the very label we are using. The word *information* in its name implies a direct and exclusive relationship between IO and *Information* Superiority as well as the *Information* Domain. Another contributing factor is the persistent confusion between *influence* capabilities, provided by IO, and *influence* effects, the essence of all warfare. In the end, reliance on *information* as the common denominator for this set of capabilities eventually led to IO tribalism within the Air Force and an inefficient “everything is IO” mindset.

If Air Force IO is going to provide relevant and useful engagement options to commanders, it must bring specific capabilities to the fight not already clearly defined in our air warfare, space operations, or mobility doctrine. The Air Force made significant progress by streamlining its version of IO in January 2005, but still did not clearly define a replacement for *information* as the entrance qualifier for IO doctrine. Without a common “glue” to bind these capabilities, IO is simply a conglomeration of unrelated and otherwise orphaned mission areas.

This research paper examines IO concept development over the last decade and investigates some of the problems resulting from recent Air Force IO terminology and doctrine. Based on a vision for the seamless integration of kinetic and non-kinetic capabilities, this paper proposes discarding the misnomer IO in favor of a new term, “Non-Kinetic Operations”. More than just a name change, this new label represents the glue that binds Electronic Warfare, Influence Operations, and Network Warfare Operations. By adopting Non-Kinetic Operations as the next generation of Air Force IO, we can finally focus on “Integrated Operations”, the only “IO” that really matters in joint effects based operations.

Introduction

The mind of the enemy and the will of his leaders is a target of far more importance than the bodies of his troops.

— Mao Tse-Tung

What are Information Operations and how do you achieve Information Superiority? Does successful Information Warfare lead to Information Superiority? The United States Air Force has struggled with these questions for more than a decade in an effort to operationalize Information Operations (IO) in support of Unified Combatant Commands. However, despite more than a decade of debate, IO is simply not yet a part of the Airman's mindset because we still do not agree on what it is.

On one hand, IO still does not receive sufficient attention and confidence from Air Force planners to stand on equal ground with more traditional kinetic capabilities. The air war over Kosovo demonstrates that IO is often an after-thought in the air component's planning process. Although planning for Operation ALLIED FORCE began nine months before the start of the conflict on 24 March 1999, Secretary of Defense William Cohen testified before the Senate Armed Services Committee "the conduct of an integrated information operations campaign was delayed by the lack of both advanced planning and strategic guidance defining key objectives." This clearly implies that IO was not an important part of initial campaign planning.¹

On the other hand, much of the prevalent hype in recent staff briefings across the Air Force suggests that IO is a military panacea incorporating a disparate collection of capabilities.² As recent as December 2004, Air Force Doctrine Document (AFDD) 2-5 defined IO to include Computer Network Operations, Psychological Operations (PSYOPS), Electronic Warfare (EW), Operational Security (OPSEC), Intelligence, Weather, Precision Navigation, Special Operations

and even Physical Attack for influence effect.³ In other words, if it had anything to do with *information*, it was part of Information Operations. Using this model, it was difficult to determine what military capability was not an *Information* Operation. Applying this faulty dilemma to other mission areas, we would have to categorize bullets fired from an infantryman's rifle and ship-to-ship missiles employed by the Navy as *Air Operations* because the bullet and the missile travel through the air. At this extreme, the question then becomes "If everything we do in the military is an Information Operation, what value is the label? Why not just call it operations?"

So if *information* itself is not the common denominator for this doctrinal set of capabilities, then what is it? What is the glue that binds these seemingly unrelated capabilities together? Although entirely appropriate for an immediate post-Cold War environment, characterized by diminishing defense budgets and increasing military deployments, the IO paradigm is currently outdated and in need of a conceptual overhaul. The January 2005 release of AFDD 2-5 goes a long way towards operationalizing this mission area, but still does not clearly define the binding agent for what we now call Information Operations.

This research paper examines the problems associated with recent Air Force IO terminology and doctrine, and promulgates a vision for Air Force IO focused on the seamless integration of kinetic and non-kinetic capabilities. The methodology for this examination begins with contextual and literal definitions of IO, and then looks at how this mission area has developed over the last decade, followed by the conceptual deconstruction that led to the current doctrinal construct. The paper will culminate with a modified vision for Air Force IO and a proposal to label this set of capabilities "Non-Kinetic Operations", further suggesting that the "IO" we should concern ourselves with is actually "Integrated Operations".

Defining Information Operations

You keep using that word... I do not think it means what you think it means.

— Inigo Montoya to Vizzini
From the movie “The Princess Bride”

If you asked a dozen people to define *Information Operations*, you would likely get a dozen different answers.⁴ Information Operations often conjures images of cyber warfare and mind control. Is it simply operating with information? Is it predominately non-kinetic operations? When do Information Operations become Information Warfare? Is IO the direct and exclusive means of attaining Information Superiority? How do you know when you have achieved Information Superiority? Before establishing a vision for the future of Air Force IO, we must first understand the terminology involved. This paper will address these questions by examining the differing service perspectives, the domains in which they operate, and finally the terminology of IO itself.

Complicated by Tribal Perspectives

The first problem with defining Information Operations is the differing opinions of what military actions actually comprise it. Joint Publication 3-13 offers a joint definition for IO based on strategies and capabilities to affect information and information systems.⁵ However, each service branch has tailored its own version of IO to best suit their parochial needs. The Army focuses on employing IO as an element of combat power to achieve information superiority at decisive points in an operation, in order to support the commander in seizing, retaining, and exploiting the initiative.⁶ This translates to heavy emphasis on Army IO elements such as PSYOPS, Deception, OPSEC and related activities like Public Affairs and Civil Military

Operations. The Marine Corps views IO as an enabling and enhancing function to support Expeditionary Maneuver Warfare.⁷ Marines use IO to integrate command and control, fires, maneuver, logistics, intelligence and force protection. Placing heavy emphasis on areas like Electronic Warfare and Information Technologies, the Navy takes more of a Network-Centric Warfare approach by using Information Operations to affect adversary and protect friendly decision-making capabilities.⁸

Even within the Air Force itself, there are many tribal perspectives of IO, most of which are completely out of synchronization. Different Air Force specialties tend to focus on their specific role in IO. Air Force communicators tend to focus on the Computer Network Defense and Information Assurance components of IO.⁹ The intelligence community typically centers on the information gained and exploited through employment of intelligence, surveillance, and reconnaissance capabilities.¹⁰ Weary from nearly 30 years of under-funding, Electronic Warfare advocates cannot decide if IO will help or hurt their future status as a legitimate mission area. Of course, Space proponents concentrate on the counter-space relevance of IO and the Airlift community defends its often forgotten applications for Military Operations other than War (MOOTW). Public Affairs desperately wants to participate in IO, while simultaneously establishing a distinct firewall between itself and influence operations like PSYOPS and military deception. The Office of Special Investigations must periodically remind us all that counter-intelligence is also a valid element of IO. Even the lawyer and chaplain can explain how they make significant contributions to a particular slice of Air Force IO. With so many diverse perspectives, it is no surprise the Air Force struggles with how to define its role in Joint IO.

All of the services, including the Air Force, perceive IO as a means to enhance their particular scheme of maneuver. However, as was the case with long-range bombing, the Air

Force also tends to see strategic possibilities for IO, especially for Influence and Network Warfare capabilities. Given the different service viewpoints, is IO only a force enhancer like intelligence and communications? Is it an exclusive means for attaining Information Superiority on the battlefield? Is it a unique set of engagement options made available to the Joint Force Commander (JFC)? Although sometimes difficult to integrate in joint operations, all of these are reasonable perspectives considering the respective domains within which each of the military services operates.

The Information Domain

Each of the U.S. military branches lays claim to a particular physical domain. The Army conducts fires and maneuvers on land. The Navy operates from the sea. The Air Force operates in the air and space domains. However, 21st century commanders must also consider the cognitive and information domains.¹¹ The cognitive domain is the medium where people's thoughts, personalities, values, and beliefs exist. Linking this to Col John Boyd's OODA Loop, the cognitive domain is where military leaders on both sides of a fight *orient* what they observe on the battlefield and *decide* how to act on it.¹² As paraphrased from Mao TseTung's writings, the mind of the enemy commander, his cognitive processes, are the principle military target. However, we cannot directly target the cognitive domain and change an enemy's mind for him. We can only change the environment in which he exists.

The information domain provides the connection between the physical and cognitive domains. All activities in the physical domain create effects in the cognitive domain, provided someone *senses* the activity. This brings to mind the classic dilemma, "If a tree falls in the forest and nobody is around to hear it, does it make a sound?" Information provides a cognitive lens to

the physical domains. In a military context, the information domain is the medium through which we can change the enemy's perceptions of the battlefield, disorient him, and influence him to make decisions in our favor. Of course, a thinking, reacting adversary will attempt to do the same to us. This mutual desire to create effects in the cognitive domain through manipulation of the information domain suggests that information itself is a weapon as well as a target.

This realization regarding the information domain formed the basis of the Air Force's understanding of IO through 2004. This concept centered on a strategy to attack and defend information and information systems, with any physical or information-based capability available.¹³ However, this IO definition was more of a strategy than a specific set of capabilities. In effects based operations, commanders are principally concerned with the production of desired effects, not as much on the platforms or capabilities used to create them. Military force providers should offer a broad range of solutions to commanders. IO can offer viable capabilities to target the *message* as well as the *means* of information flow. However, commanders may also use kinetic capabilities to target key information systems in the physical domain, like communications nodes and control centers, to create the same effects by disrupting or reshaping messages within the information domain. Therefore, despite the implications of its label, *Information Operations* is not the exclusive means to affect the *information* domain. In this case, the terminology associated with IO has been its biggest source of confusion.

Struggling with Terminology

Another obstacle towards understanding the definition of IO is the very label assigned to it. Whether we should call this doctrinal area *Information Operations* or *Information Warfare* is a subject of periodic debate. Do we conduct *operations* in peacetime and *warfare* in conflict?

Perhaps *operations* are a subset of *warfare*, or vice versa. Joint Publication 1-02 defines *operation* as “a military action or the carrying out of a strategic, operational, tactical, service, training, or administrative military mission.”¹⁴ While this meaning for operation encompasses the entire spectrum of conflict, the term *warfare* is limited to “the waging of war.” Therefore, the term *warfare* is inherent to *operations* and not the other way around. Because it does not address the full spectrum of conflict, there is no value added by use of the term “Information Warfare”. For the purposes of this research paper, further references to “Information Operations” shall infer military actions within the subject doctrinal area during peace, transition, and war.

Information Superiority, like air superiority, is a critical element of successful joint operations. The question is, “Do successfully executed Information Operations achieve Information Superiority?” The answer is, “Yes, but not alone.” The Air Force currently defines *Information Superiority* as “the degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.”¹⁵ As previously discussed, we can create information effects using kinetic or non-kinetic capabilities. Therefore, IO is an inclusive, not exclusive, contributor to the achievement of Information Superiority.

Certainly, across the spectrum of conflict, information itself is a constant object of military pursuit as well as a lucrative target vulnerable to attack. Clausewitz regarded the role of information and knowledge in warfare as “a factor more vital than any other.”¹⁶ The American Heritage Dictionary of the English Language defines *information* as “knowledge derived from study, experience, or instruction.” For comparison, Joint Publication 1-02 defines *information* as “facts, data, or instructions in any medium or form.”¹⁷ By either definition, information is

pervasive throughout all aspects of military operations including surveillance, targeting, engagement, assessment, mobility, administration, logistics, and command and control. To some degree, *every* military activity is dependent on the interpretation and dissemination of information. Therefore, use of the term *information* in the label for this set of capabilities implies that “everything is an *Information* Operation.” Of course, when referring to IO, we did not intend for this paradox to result. However, words do have meaning and we should consider adjusting the terminology to accurately reflect our meaning.

IO is also not as simple as “operating with information”. If so, placing a phone call to order a pizza, sending an email to a friend, or even writing this paper would qualify as an Information Operation. These activities are merely things we do while operating in the information age. While PSYOPS, EW, and network defense may qualify as “operations”, the use of the word “information” misrepresents the nature and limits the utility of these capabilities. Even worse, it encourages an “everything is IO” mentality. Therefore, the label “Information Operations” may be one of the biggest misnomers in our modern military lexicon.¹⁸

Air Force Information Operations 1994-2004

In all fighting, the direct method may be used for joining battle, but indirect methods will be needed in order to secure victory.

— Sun Tzu
Circa 500 B.C.

Following the end of the Cold War, the United States military was in search of a new operational paradigm to address a changed global environment distinctly characterized by information-age technology. The rapid rate of globalization and the increasing societal dependence on information systems created a cheaper way to attack the United States without confronting its peerless military strength. This information-age version of Sir Basil Liddell-Hart's "indirect approach" suggested images of Mathew Broderick, portraying a teenager in the 1983 movie "Wargames", hacking into government information systems to initiate a global thermonuclear war. Meanwhile, uncontested success against the Iraqi military in Operation DESERT STORM validated the asymmetric advantage of gaining and maintaining Information Superiority against an adversary. In the early 1990s, Information Warfare intrigued the defense community as both a threat and as an opportunity.¹⁹

In his article "Warfare in the Information Age", Bruce Berkowitz compares "the emergence of Information Warfare with the evolution of mechanized warfare in the mid-1800s."²⁰ The Industrial Revolution introduced weapons far superior to previous military capabilities. Long-range artillery, machine guns, and steam-powered armored warships transformed warfare of the period into a faster, longer-range, and more deadly affair. More significantly, these new military technologies offered adversaries new targets within a nation's industrial base. As Berkowitz describes, the introduction of new technologies and their

associated vulnerabilities motivated a complete rethinking of how to wage war. For the last fifteen years, the United States military has largely believed the same to be true for IO.

The identification of IO as a possible revolution in military affairs does not automatically change the nature of warfare. The U.S. military has often chased promising new technologies without securing the concepts of operation and organizations required to realize its potential. Consider the invention of the rifled musket and minnie ball just before the U.S. Civil War. Despite effective ranges of hundreds of yards, both sides continued to fight using Napoleonic tactics where densely packed infantry lined up, marched to within fifty yards, and blasted each other.²¹ This failure to match a new technology with appropriate concepts and organizations proved suicidal and contributed to more than 600,000 American deaths. This number is much higher if you consider we did not really learn this lesson until after the horrors of trench warfare in World War I. In similar fashion, we will waste the potential of IO if we fail to create meaningful doctrine, vision, and organizations.

There is a clear trail of evidence over the last decade to demonstrate that Information Operations is still a rapidly evolving mission area within the United States Air Force. During their tenure as the Secretary and Chief of the Staff of the Air Force from 1994 through 1997, Doctor Sheila E. Widnall and General Ronald R. Fogleman released a document entitled *Cornerstones of Information Warfare*. This official release was significant because the Air Force formally recognized IO as a potential revolution of military affairs. They defined information as a separate realm, independent from the physical domains of air, land, sea, and space. They pointed to information as a potential weapon as well as a lucrative target. While this was a crucial first step in officially defining this emerging mission area, it also established a mindset that would prove difficult to overcome over the next decade. In the mid-1990s, this Air Force

publication defined Information Operations as “*any action* (emphasis added) involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces.”²² In the mid-1990s, this idea firmly planted the idea that “everything is IO” into the Airman’s mindset.

By January of 2002, the Air Force further evolved its IO doctrine by integrating all mission areas associated with attacking and protecting information and information systems. As illustrated in Figure 1, the 2002 version of Air Force IO was broken into three major parts.²³

Information Warfare (IW) included the major IO capabilities used to attack and defend information and information

systems. Information-In-Warfare (IIW) provided military activities that gain and exploit information such as Intelligence, Surveillance, and Reconnaissance (collectively

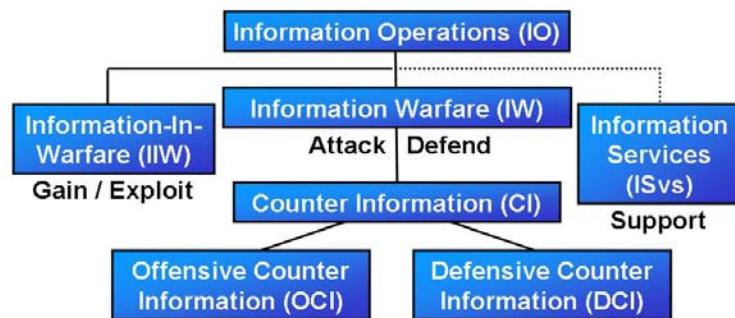


Figure 1: Air Force IO Construct (2002).

known as ISR), Weather, Public Affairs (PA), and Precision Navigation and Positioning (PNP).

Information Services (ISvs) provided the communication backbone that enabled the command and control system we depend on to execute Air, Space, and Information capabilities around the world. Both IIW and ISvs are vital to *all* Air Force operations, but neither is exclusive to IO. They were included in IO alongside IW because, in 2002, the entrance qualifier for IO was still the word “information”.

This 2002 construct pulled together every information-based capability and established IO as “those operations that achieve and maintain Information Superiority.”²⁴ In addition to IIW and ISvs, these capabilities included PSYOPS, Computer Network Operations, EW, Military

Deception, Information Assurance, Operational Security (OPSEC), and even Physical Attack for influence effect. By laying claim to all of these capabilities, a skeptical mind must question what capabilities would NOT fall under this 2002 version of Air Force IO. There was no requirement to integrate IO with other military

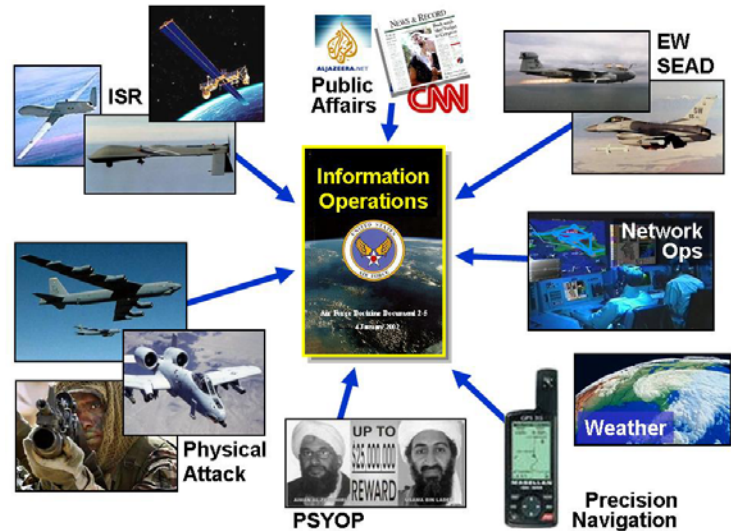


Figure 2: Everything is IO (2002).

mission areas; it was in itself an integrating strategy. In effect, at the turn of the century we had built Air Force IO into a stand-alone, self-integrating construct that only perpetuated the “everything is IO” mentality (Figure 2). It also resulted in command and control impossibilities. After all, whoever controlled this version of IO would theoretically control everything, right?

Despite the unwieldy nature of the 2002 version of Air Force IO, it did offer a couple lasting benefits. First, this evolution of IO did help operationalize the Air Force intelligence and communications communities by giving them a mission area with great potential to produce military effects. This was important for IO development given the operational community’s tendency to ignore unfamiliar non-kinetic capabilities in favor of the more familiar kinetic options. Unfortunately, both communities focused primarily on the gain-exploit-attack-defend cycle in Computer Network Operations and could not adequately address EW or the full range of influence-based operations. Portions of the intelligence community, particularly from the Air Intelligence Agency, long argued to keep ISR embedded within IO. Their intent was to keep the Gain-Exploit-Attack-Defend continuum coherent within a single doctrinal document.²⁵ Instead

of embracing the entire family of Air Force doctrine as their own and relying on operational integration to bring capabilities together, they were effectively building a ‘one-stop-shop’ doctrinal document for this continuum.

A second benefit of this construct was a much-needed “de-mystification” of IO after 2002. The global and unpredictable nature of certain IO capabilities, real or hyped, often resulted in planners treating the entire IO construct as a nuclear weapon. Intimidated by its mythical potential and technological fragility, few Airman were brave enough or understood IO well enough to employ it in training or contingency. Furthermore, if the “effects” IO capabilities can provide the Joint Force Commander do not make the planning table, they will not be relevant in the future. Although many IO capabilities are now coming out from “behind the green-door”, we must avoid over-classifying sensitive capabilities while balancing the requirement to protect fragile technologies.²⁶ Essentially, the 2002 iteration of IO was essential to get the mainstream Air Force talking about IO today.

Fortunately, we are now smarter with more than three years of combat experience engaged in the Global War on Terrorism. The Air Force today, like the rest of the joint community, understands better than ever that IO can make significant contributions to the joint fight. After a difficult year of debate and compromise, the Air Force finally released an updated version of its doctrine for Information Operations in January 2005. The development of this latest iteration of AFDD 2-5: *Information Operations* clearly signaled the end of the “everything is IO” mentality by tearing down the IO stovepipes erected over the last decade.

Tearing Down IO Stovepipes

Adherence to dogmas has destroyed more armies and cost more battles than anything in war.

— J.F.C. Fuller

Many people erroneously refer to IO as if it were a standalone capability. IO is merely a label to describe a unique collection of capabilities offering potential military solutions to commanders. Across the joint community, we already have doctrine associated with military operations in the physical domains of air, space, land, and maritime. Special Operations doctrine spans many of these domains, but we do not want to treat IO as “special”. Instead, we must normalize IO by refining our doctrine and concepts of operation in such a way that our people can understand it, our force providers can posture it, and our commanders have the confidence to employ it.

Air Force Basic Doctrine, entitled AFDD 1, calls for Airmen to focus on integration, not just synchronization.²⁷ This means we cannot be satisfied with the mere deconfliction of joint forces, as was the case with route packages in Vietnam, for example.²⁸ *Integration*, by comparison, is “the arrangement of military forces and their actions to create a force that operates by engaging as a whole.”²⁹ To be meaningful in this jointly integrated context, Air Force IO cannot be the panacea espoused in previous Air Force doctrine. IO must provide specific, unique, and useful capabilities to the JFC. With this in mind, we can start taking apart the 2002 Air Force IO model and see if we can put it back together in a more operationally relevant construct. Be warned, just like taking apart an engine in your garage, there might be extra parts at the end that just do not seem to fit into the rebuilt version.

Why did Airmen believe in the previous “everything is IO” construct? The answer is simple, “it was in our doctrine.” Therefore, the first step is to subject Air Force IO doctrine to a weight loss program of sorts.

The “Less is More” Approach to Information Operations

As previously discussed, both IIW and ISvs are vital to *all* Air Force operations, and therefore neither is exclusive to IO. We must “Gain and Exploit” adversary information to successfully employ any military “Attack and Defend” capability. For this reason, we pulled IIW and ISvs out of the 2005 Air Force IO construct.³⁰ This in no way devalues capabilities like ISR, but rather recognizes their critical relevance to all operations. Although we promoted the larger ISR out of IO doctrine, we must recognize the inextricable linkage of a few dedicated and tailored gain and exploit capabilities. Without Electronic Support, there can be no Electronic Attack or Protect; and without network surveillance and exploitation, there can be no Network Warfare Attack or Defense. Although less mature, we should also recognize influence support capabilities that enable influence operations. This is where Foreign Area Officers, socio-analysts, theologians, and inter-agency partnerships may come into play. Without these specialized ISR capabilities, there would be no IO.

After trimming IO down to just its offensive and defensive capabilities, we cannot just leave IIW and ISvs lying on the garage floor. Fortunately, finding logical homes in Air Force doctrine for most of these capabilities is easy. We already have a strong concept for Combat Support doctrine that includes maintenance of our Air Force networks and the “base-newspaper” side of Public Affairs.³¹ Weather and Precision Navigation and Positioning could also find logical homes in Combat Support doctrine.

Command, Control, Intelligence, Surveillance, and Reconnaissance, collectively referred to as C2ISR, all provide key skill-sets to the joint fight, but they are not all of equal importance. According to General Hal M. Hornburg, a former Commander of Air Combat Command, the most important is *control*. Combined with C2 and Battle Management systems, ISR capabilities contribute to the essential science of *Control*, which in turn enables the art of *Command*.³² This justifies removing ISR from under IO and establishing it in a separate doctrinal document, AFDD 2-9 for example, or merging it with C2 to form an integrated AFDD 2-8 *C2ISR* volume.³³ Regardless, we must find a home for ISR that accurately captures its essential contribution to all Air Force capabilities.

With IIW and ISvs removed from the IO construct, we streamlined the previous version of IO down to just Information Warfare (IW). While we certainly conduct information operations during war, the term IW fails to recognize the operational role of these capabilities during peacetime, contingency, pre- and post-conflict situations. In fact, the Air Force conducts IO every day of the year by protecting our networks from intrusion and assuring the integrity of military information and information systems. Therefore, as done in this paper, the authors of the 2005 version of Air Force IO also discarded the term Information Warfare.³⁴

While finding new doctrinal homes for IIW and ISvs, we can now sort through the remaining capabilities including EW, Computer Network Operations, PSYOPS, Counter-Intelligence, Counter-Propaganda, OPSEC, PA, Military Deception, and Physical Attack. Of all these, the latter is the most glaring source of the “everything is IO” perspective. The 2002 version of AFDD 2-5 discusses how cruise missiles, combat aircraft, special ops teams, and precision guided munitions may be construed as an Information Operation due to the effect that they may have on their target.³⁵ This subordination of physical attack under IO is a flawed

construct for two reasons. First, subordinating physical attack capabilities into two doctrinal constructs encourages tribalism. Airmen should claim the entire family of Air Force doctrine as their own, as if it were one big book, instead of narrowing in on a particular chapter associated with their particular tribe. This family of doctrine approach is important for operational integration. Second, the heart of this misunderstanding about Physical Attack's relationship to IO stems from confusion between capabilities and effects.

Capabilities and Effects

We have made substantial progress in transitioning from metrics-based operations to effects-based operations. However, the Air Force itself, as a military service, does not produce direct combat effects. Instead, we organize, train, and equip capabilities and grow leaders who know how to employ them. We then provide both of these as combat potential to the Unified Combatant Commands. This combat potential might be iron on the ramp provided as Air Expeditionary Task Forces, or reachback forces that can produce and support combat effects from the Continental United States. Of course, all of these forces include Airmen doing what the Air Force has trained and equipped them to do, but now they produce combat effects, typically under the operational control of a JFC.³⁶

The power of the Joint Force stems not only from the high-tech nature of our weapon systems and the tireless training we give our servicemen and women, but also from the broad range of capabilities combatant commanders have at their disposal to solve real military problems. Certainly, Information Operations puts some of these arrows into the commander's quiver of options. However, physical attack in the form of "hard-kill" or kinetic weapons may also to contribute to the desired *influence* effects. This does not mean physical attack, a B-52

strike for example, is an influence capability, nor does it mean we should doctrinally compartmentalize physical attack under Information Operations. More specifically, we must recognize the difference between influence capabilities, like PSYOPS and Military Deception, and influence effects, which are the essence of all warfare.

The Essence of Warfare

Military forces have employed some form of Information Operations since the dawn of human conflict. As early as 500 B.C., Sun Tzu wrote, “All warfare is based on deception.”³⁷ At the heart of all warfare is the desire for one group to influence another group. Conflict between nations could be about land, power, trade, ethnic or religious differences, but the desired effect is always about influencing the other side to capitulate in some way. The stated goal of Operation LINEBACKER II was to influence the North Vietnamese to return to the negotiation table. In Operation DESERT STORM, we sought to influence the immediate, unconditional, and complete withdrawal of all Iraqi forces from Kuwait. Finally, a primary objective in our Global War on Terrorism is to influence peaceful nations, even weak and failing states that may need our assistance, to deny terrorist organizations the breeding ground they need to expand their networks. Because “everything really is for influence *effect*” and IO includes many obvious influence *capabilities*, the “everything is IO” trap threatens to ensnare us again.

As a military service, the Air Force organizes, trains, and equips influence “capabilities” that commanders may employ to achieve influence “effects”. However, kinetic capabilities like close air support and air interdiction are air operations that may also contribute to the desired influence “effect”. Some have argued the B-52 is a psychological weapon because we used it to influence Iraqi forces to surrender in 1991 during Operation DESERT STORM. Although

catchy, this statement is doctrinally flawed. This is the same as concluding, “A screwdriver is a heating capability because friction warms the screw as it is turned.” The screwdriver simply provides the capability to turn a screw. Second order effects, like heat generated by friction, can be either inconsequential or a desirable and useful byproduct of the employed capability.

In Operation DESERT STORM, we used specific influence capabilities such as PA and PSYOPS to educate Iraqi citizens and soldiers about the power of American bombers and our intent to use them. Well-timed B-52 strikes near Republican Guard armored columns added significant credibility to these influence capabilities and produced an integrated effect more substantial than either separate capability might have generated. In similar fashion, potential adversaries respect American airpower thanks to the application of influence capabilities around the world. This speaks to the power of operational integration to produce desired effects and achieve commander’s intent. It is no accident that “Integrating Operations” is one of our three Air Force core competencies.³⁸

Influence is the essence of all warfare. IO provides dedicated “influence capabilities” to commanders, but they are not restricted to these “influence capabilities” in order to produce the necessary “influence effects”. The commander can choose numerous paths to get to the same result. Factors like collateral damage, political impact, operational risk, speed, cost, and security may help the commander select the right combination of kinetic and non-kinetic capabilities for employment. Therefore, although victory in warfare may require achievement of certain “influence effects”, we can conclude that *not* everything is an Influence Operation.

Recommending a New Vision for USAF Information Operations

We need to be able to think in terms of target effects. I picture myself around that same targeting table where you have the fighter pilot, the bomber pilot, the special operations people, and the information warriors. As you go down the target list, each one takes a turn raising his or her hand saying, I can take that target.

— General John P. Jumper
Commander, USAFE
25 Mar 1999

If Air Force IO is going to provide relevant and useful engagement options to commanders, it must bring specific capabilities to the fight not already clearly defined in our air warfare, space operations, or mobility doctrine. In other words, we must define the unique qualifier that defines entry into the Air Force IO doctrine. As argued in this paper, our experience over the last ten years has already demonstrated the trap resulting from simply relying on the word “information” as this qualifier. At the same time, Information Operations should not end up the final resting place for capabilities that just did not fit in other, more mature, mission areas. We must define the glue that binds this set of capabilities.

Relevance for IO is contingent on the needs of the JFC. Stovepiped capabilities that do not integrate well with other joint capabilities are not useful in joint effects-based operations. The commander must integrate a broad range of military disciplines so that the total military potential at his fingertips is greater than the sum of its parts if employed in a “disjointed” manner. This entails a focus on effects, independent of platforms and parochialism. In selecting specific capabilities to produce desired effects, planners will consider elements of the operational art, the principles of war, the principles of MOOTW, and factors like collateral damage, and the Law of Armed Conflict.³⁹ Under pressure, a JFC will tend to select capabilities based on confidence acquired in testing and training. This will require us to treat IO capabilities like

weapon systems by applying standards for testing, evaluation, training, and technology. In the end, IO must be a specific set of capabilities that we could integrate with other joint capabilities to produce effects based operations in support of the JFC.

The newest version of AFDD 2-5: *Information Operations*, released in January 2005, removes Information in Warfare, Information Services, and Physical Attack from Air Force IO. Under this new construct, the goal of Air Force IO is to “influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.”⁴⁰ The core IO capabilities of Electronic Warfare, Network Warfare Operations, and Influence Operations provide engagement options able to “influence, disrupt, corrupt, or usurp”. This new doctrine further expands Influence Operations into six sub-capabilities including PSYOPS, Military Deception, OPSEC, Counter-Intelligence, Counter-Propaganda, and PA Operations. All of these are unique and operationally useful capabilities not specifically found in other doctrine. Furthermore, joint planners could feasibly integrate any of these capabilities into the JFC’s campaign. These capabilities each carry unique collateral damage and targeting considerations, essentially allowing IO capabilities to bypass traditional fielded forces to affect an adversary’s vulnerable centers of gravity. It seems the latest version of AFDD 2-5 finally provides a relevant model for Air Force IO by using a “less-is-more” approach for inclusion of capabilities.

However, this latest version of AFDD 2-5 still does not clearly define the glue that unifies these capabilities under the IO umbrella. It does concede, “IO provides predominantly non-kinetic capabilities to the warfighter.”⁴¹ Use of the word *predominately* in this statement was clearly a compromise, begging the question, “Which of these IO capabilities are then kinetic by nature?”

Making the Case for Non-Kinetic Operations

Influence Operations are intuitively non-kinetic. PSYOPS, Military Deception, and PA Operations all target the cognitive domain to influence an adversary or inform a global audience. Some may argue that the distribution of leaflets, dropped by fighter aircraft in converted bomb casings, qualifies as a kinetic capability. This is muddled thinking. Indeed, the bomb casing and even the leaflet itself is technically mass in motion. However, the bomb casing, paper, and aircraft constitute delivery platforms, not capabilities. The capabilities provided by Influence Operations are ways of influencing decisions, behaviors, perceptions, or attitudes of a target audience ‘non-kinetically’, using PSYOPS, Military Deception, and PA Operations.

Electronic Warfare advocates may argue that towed-decoys, chaff, and flares are kinetic ‘capabilities’. This is not true. Again, they are indeed kinetic ‘platforms’, again involving mass in motion. The capability these EW platforms provide involves the manipulation of radar waveforms to produce false targets on an adversary’s radar screen; this is clearly a non-kinetic capability. Some may also contest that EW is kinetic when it comes to employment of the High-speed Anti-Radiation Missile (HARM). Although extremely EW dependent, HARM is not EW. It is one of many platforms supporting Offensive Counter Air capabilities. The Suppression of Enemy Air Defenses (SEAD) is the perfect cross-doctrinal case for operational integration. Our Air Warfare doctrine provides Lethal SEAD through employment of physical attack, including HARM or iron bombs, while EW provides Non-Lethal SEAD through employment of electromagnetic attack.⁴² Synergistically employed, Lethal and Non-Lethal SEAD constitute a range of options to neutralize, destroy or disrupt enemy air defenses.

The kinetic debate “heats up” even more in regards to the use of lasers and high-power microwave, both of which fall under the common definition of EW.⁴³ According to the

American Heritage Dictionary, laser is actually an acronym standing for “L(ight) A(mplification by) S(timulated) E(mission of) R(adiation).” Additionally, microwave is “electromagnetic radiation between infrared and shortwave radio wavelengths.” Although lasers and microwaves can heat up conductive targets to the point of rupture or explosion, their electromagnetic nature implies they are non-kinetic. If the laser or microwave is used to affect an adversary’s use of the electromagnetic spectrum, or protect our ability to do so, then it is indeed a non-kinetic capability under EW. However, if it is used to blow up ballistics missiles for example, it is a Defensive Counter Air capability conducting Theater Ballistic Missile Defense. The capability, not the platform, determines whether it is kinetic or non-kinetic in nature.

Conceptually speaking, Network Warfare advocates may argue the ability to burn up a hostile computer system is a kinetic capability. This is also not true either. A notional ‘cyber’-capability to remotely shut off a computer’s cooling fan or send a hard drive into catastrophic failure is a matter of electronic signals sent across data networks. As second or third order effects, these capabilities could destroy a motherboard, the entire computer, or even the adversary building that housed the computer. However, based on the means used to achieve the first order effect, it is clear that the capability itself is strictly non-kinetic by nature.

IO gives commanders new ways to attack existing targets, and in some cases like Network Warfare Attack, new ways to attack new targets. However, we must keep the difference between capabilities and effects clear. Although IO capabilities may produce lethal second or third order effects, they are all inherently non-kinetic engagement capabilities. So finally, we have a useful construct where IO is a set of non-kinetic engagement capabilities that support effects-based operations by providing additional solutions to commanders for dealing with real military problems. To represent this set of capabilities accurately, the Air Force should

abandon the term “Information Operations” and its associated baggage in favor of the new, more accurate label, “Non-Kinetic Operations” (Figure 3).

This proposal represents more than just a name-change for IO. The first benefit of Non-Kinetic Operations is that is simply easier to understand. If it is easy to comprehend how these capabilities fit into the Air Force’s contribution to joint warfighting, it will

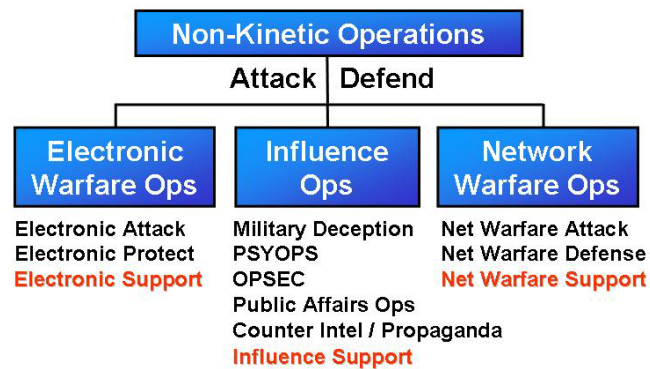


Figure 3: Non-Kinetic Operations (2005).

finally become part of the Airman’s mindset alongside air and space power. People commonly associate the military instrument of power with traditional “blast, heat, and frag”. However, the military’s role in support of the informational instrument of power is more confusing. By trading the IO label for Non-Kinetic Operations, we will clarify how these Air Force capabilities, as part of the military instrument of power, can create effects across the entire D-I-M-E.⁴⁴

A second benefit is the further demystification of these capabilities. By name alone, Non-Kinetic Operations may prove more approachable than IO or IW when working with Congress to secure funding for new capabilities. Additionally, the integration of Non-Kinetic Operations may also mitigate our tendency to over-classify and treat anything having to do with IO as if it were a nuclear weapon. These are not nukes. We can integrate the *effects* produced by Non-Kinetic Operations without compromising fragile technologies.

Finally, by narrowing the IO vision down to the more manageable concept of Non-Kinetic Operations, we can also improve force development within this mission area. We have EW professionals. We also have computer network professionals. However, we are seriously

lacking in professional influence operators. The Air Force should consider the creation of a new career path, focused on supporting joint influence objectives through employment of skills like PSYOPS, OPSEC, and Military Deception. Finally, we must bring these otherwise divergent career paths together, along with our kinetic experts, in the Air and Space Operations Center to ensure we integrate Non-Kinetic Operations at the operational as well as tactical levels of war.

Information Superiority

If the Air Force were to replace the outdated IO paradigm with a new vision for Air Force Non-Kinetic Operations, what are the implications for Information Superiority? We can answer this question by examining Air Superiority. Air operations are not the exclusive enablers for Air Superiority. Under integrated joint operations, kinetic and non-kinetic engagement capabilities may all contribute to Air Superiority. Such is the case with Information Superiority. Although Non-Kinetic Operations may provide some of the obvious means to attack adversary or defend friendly information systems, we may achieve similar effect through the application of Kinetic Operations from any of the physical domains. For example, the Joint Forces Commander may require a hostile integrated air defense system neutralized to reduce adversary situational awareness and allow safe passage for humanitarian operations. Joint planning options may include electronic jamming, computer attack, PSYOPS targeting of missile operators, or some sort of Military Deception plan. However, a cruise missile attack, a B-52 strike, or a Special Operation employed in direct action against key command and control nodes or early warning radars may achieve similar effect. In fact, an Army Stryker unit occupying a hostile missile site suppresses that portion of the enemy's air defenses as effectively as any other capability. By normalizing Non-Kinetic Operations with other Air Force capabilities to achieve air, space, and

information superiority, it becomes more relevant and useful to commanders as a legitimate set of options to solve real military problems. Therefore, we achieve *Information Superiority* through the employment of the full range of “integrated” joint operations, not just so-called *Information Operations*.

After clarifying the entrance qualifications for Air Force IO, we have a coherent operational concept that will run on all cylinders. Instead of a self-integrating, stand-alone concept that encompasses everything, this proposal for Non-Kinetic Operations provides unique engagement options for the commander’s bag of tricks. This modification of Air Force IO provides legitimate and useful non-kinetic capabilities that we can integrate with all other joint capabilities.

At the end of the day, ‘Integrated Operations’ is the true Holy Grail we have long searched for. Non-Kinetic Operations, as the next evolution of Information Operations, is an important component of the Airman’s contribution to joint warfighting. Non-Kinetic Operations fits well alongside Air Warfare, Space Operations, MOOTW, Combat Support, Air Mobility Operations, and Special Operations as chapters in the family of Air Force Doctrine (Figure 4). As is the case with Air Superiority, all of these operations may collectively contribute to Information Superiority.

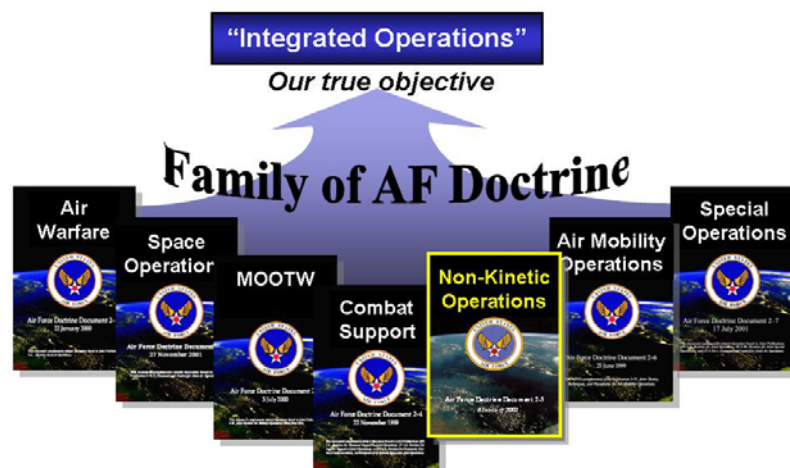


Figure 4: The Family of AF Doctrine.

Conclusion

We thought we were introducing into the world an invention which would make further wars practically impossible...

In a research paper on Air Force Information Operations, the quote above seems very applicable to the potential utility of Information Operations as a surrogate for conventional war. Conjuring visions of hacker versus hacker in a cyber struggle for global dominance, Information Operations seems to offer the promise of a bloodless means for future nation-states to resolve their conflicts. As is the case with Information Operations, this quote captures the American tendency to over-hype certain new technologies as the next revolution in military affairs. However, this quote is over 90 years old, and had nothing to do with Information Operations.

(continued)... Nevertheless, the world finds itself in the greatest war in history. Neither side has been able to win on account of the part the aeroplane has played.

— Orville Wright
17 June 1917

Despite the early thoughts of the Wright brothers, or the dark predictions of Giulio Douhet, air warfare did not make land or maritime warfare obsolete. Given the evidence provided by two world wars and countless regional conflicts, the invention of the airplane certainly did not make war in the 20th Century impossible. However, the integration of airpower did significantly transform the way nations have fought every war since its invention. The same is undoubtedly true for the future of Information Operations.

Since the mid 1990's, the Air Force has aggressively pursued an understanding of how Information Operations can change the nature of warfare in the post-Cold War environment. Air

Force IO grew from emerging information technologies and was initially tied to the exclusive attainment of Information Superiority. Despite its flawed “everything is IO” premise, the previous iteration of Information Operations did help operationalize the Air Force intelligence and communication communities by giving them a weaponized mission area to call their own. While this breathed new life into these individual tribes, it missed the mark in posturing relevant capabilities for employment by the Joint Force Commander. Relevance, in this case, requires the mission area to bring unique and useful capabilities to the planning table for integration into the joint fight. However, IO quickly became an operational panacea encompassing any capability dependent on information.

The latest Air Force IO doctrinal revision, culminating with the Chief of Staff’s signature in January of 2005, finally narrowed Air Force IO down to the three unique core capabilities of Electronic Warfare, Influence Operations, and Network Warfare Operations.⁴⁵ Recognition of this new vision is already gaining significant traction. Information Operations is a recurring topic at four-star Air Force conferences⁴⁶, a specialized studies course at the Air Command and Staff College, and an elective course at the Air War College.⁴⁷

By removing Information-in-Warfare and Information Services from Information Operations, the Air Force no longer relies on “information” as the entrance qualifier for the concept. We finally identify IO as a set of capabilities, spawned out the Information Age, which is unique and specific enough to be useful as a member in the family of Air Force Doctrine. While supportable, this new doctrinal approach still does not specifically define the binding characteristic that defines Information Operations. Without a common “glue” to define this set of capabilities, IO is simply a conglomeration of unrelated and otherwise orphaned mission areas. However, there is a common denominator between EW, Influence Operations, and

Network Warfare Operations. All three provide *non-kinetic capabilities* by their very nature, but possess the capacity to create lethal, non-lethal, or even kinetic *effects* in the battlespace.

Therefore, the Air Force should replace the misnomer “Information Operations” with the title “Non-Kinetic Operations” to capture the capabilities involved more accurately.

Our ultimate goal is to seamlessly integrate kinetic and non-kinetic capabilities to present the Joint Force Commander with a wide range of legitimate options to solve real military problems. Discarding the outdated label *Information Operations* in favor of *Non-Kinetic Operations* is more than just a name-change. Not only does it drop the baggage associated with the word *information*, it also recognizes the relevance of integrating meaningful non-kinetic capabilities into the joint fight and allows us to turn our attention to some of the more difficult challenges for this mission area including over-classification and force development issues. Meanwhile, with these proposed adjustments to the January 2005 release of AFDD 2-5, the Air Force will finally have its non-kinetic cursor on target.

Bibliography

- Air Force Doctrine Document (AFDD) 1. *Air Force Basic Doctrine*, 17 November 2003.
- Air Force Doctrine Document (AFDD) 2. *Organization and Employment of Aerospace Power*, 17 February 2000.
- Air Force Doctrine Document (AFDD) 2-1. *Air Warfare*, 22 January 2000.
- Air Force Doctrine Document (AFDD) 2-4. *Combat Support*, 22 November 1999.
- Air Force Doctrine Document (AFDD) 2-5. *Information Operations*, 4 January 2002.
- Air Force Doctrine Document (AFDD) 2-5. *Information Operations*, 11 January 2005.
- Alberts, David, et al. *Understanding Information Age Warfare*. Washington DC: National Defense University Press, 2001.
- Arquilla, John; Ronfeldt, David. "Information, Power, and Grand Strategy: In Athena's Camp – Section 1." 1996. Reprint, *In Athena's Camp: Preparing for Conflict in the Information Age*, National Defense Research Institute (RAND), 1997.
- Berkowitz, Bruce D. "Warfare in the Information Age." 1995. Reprint, *In Athena's Camp: Preparing for Conflict in the Information Age*, National Defense Research Institute (RAND), 1997.
- Buchan, Glenn. "Information War and the Air Force: Wave of the Future? Current Fad?" Project AIR FORCE (RAND), March 1996.
- Clancy, Tom; Horner, Chuck, General, USAF (ret); *Every Man a Tiger*, New York, NY, G. P. Putnam's Sons, 1999.
- Field Manual (FM) 3-13, *Information Operations: Doctrine; Tactics, Techniques, and Procedures*, November 2003.
- Joint Publication (JP) 3-0. *Doctrine for Joint Operations*, 10 September 2001.
- Joint Publication (JP) 3-13. *Joint Doctrine for Information Operations*, 9 October 1998.
- Navy Warfare Publication (NWP) 3-13. *Navy Information Operations*, June 2003.
- Sun Tzu. *The Art of War*. Edited by James Clavell. New York, NY: Dell Publishing Co., Inc. September 1988.
- Thomas, Timothy L. "Is the IW Paradigm Outdated? A Discussion of U.S. IW Theory." *Journal of Information Warfare*, Pages 109-116, 2003.

Thomas, Timothy L. "Kosovo and the Current Myth of Information Superiority." *Parameters*, Pages 13-29, Spring 2000.

Widnall, Sheila and Fogleman, Ronald. *Cornerstones of Information Warfare*, United States Air Force, Published between 1994 and 1997, n.d.

Weir, William R. *Turning Points in Military History*. New York, NY: Kensington Publishing Corp., March 2005.

Notes

¹ Thomas, Timothy L. "Kosovo and the Current Myth of Information Superiority." *Parameters* (Spring 2000): 13. Secretary Cohen testified to the SASC on 12 Oct 1999.

² *Recent staff briefings throughout the Air Force* is based on the author's experience as an action officer on the ACC Commander's Action Group from Aug 2002 to Jul 2004. In this capacity, the author participated in IO briefings from ACC, AFDC, AIA, AFIWC, AFSC, NSA, AFOSI, DISA, 8 AF, AMC, AFSPC, SAF/PA, HQ AF (XOI and XOR), RAND Corporation, and a host of operational units all espousing a particular view of Air Force Information Operations.

³ Air Force Doctrine Document (AFDD) 2-5. *Information Operations* (4 January 2002): 18. This version was replaced in January 2005, therefore its contents represented the Air Force view of IO through December 2004.

⁴ "If you asked a dozen people..." is based on comments by General Hal M. Hornburg, former COMACC, during his opening remarks at the December 2002 IO Summit, held at HQ AIA.

⁵ Joint Publication (JP) 3-13. *Joint Doctrine for Information Operations* (9 October 1998): vii.

⁶ Field Manual (FM) 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures* (November 2003): v.

⁷ Navy Warfare Publication (NWP) 3-13. *Navy Information Operations* (June 2003): 1-2.

⁸ Ibid., 1-3.

⁹ *Communicators* refers primarily to officers assigned the 33S Air Force Specialty Code (AFSC).

¹⁰ *Intelligence community* refers primarily to officers assigned the 14N AFSC.

¹¹ Alberts, David, et al. *Understanding Information Age Warfare* (Washington DC: National Defense University Press, 2001) as adapted for use in AFDD 2-5, *Information Operations* (2005): 3.

¹² The author proposes the link between Alberts' domain theory and Col Boyd's Observe-Orient-Decide-Act (OODA) Loop.

¹³ Air Force Doctrine Document (AFDD) 2-5. *Information Operations* (4 January 2002): 11.

¹⁴ Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms* (12 April 2001): 309.

¹⁵ Air Force Doctrine Document (AFDD) 2-5. *Information Operations* (11 January 2005): 1.

¹⁶ Arquilla, John; Ronfeldt, David. "Information, Power, and Grand Strategy: In Athena's Camp – Section 1." *In Athena's Camp: Preparing for Conflict in the Information Age* (National Defense Research Institute, RAND, 1997): 142.

¹⁷ Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms* (12 April 2001): 202.

¹⁸ General Hornburg offered the idea of *IO as a misnomer* during an office interview by the author in the Spring of 2004.

-
- ¹⁹ Berkowitz, Bruce D. "Warfare in the Information Age." *In Athena's Camp: Preparing for Conflict in the Information Age* (National Defense Research Institute, RAND, 1997): 175.
- ²⁰ Ibid., 180.
- ²¹ Weir, William R. *Turning Points in Military History* (New York, NY: Kensington Publishing Corp., March 2005): 135.
- ²² Widnall, Sheila and Fogleman, Ronald. *Cornerstones of Information Warfare*. (n.d.): 5.
- ²³ Air Force Doctrine Document (AFDD) 2-5. *Information Operations* (4 January 2002): 5.
Note: Figure 1 is the author's interpretation of IO structure and does not come from AFDD 2-5.
- ²⁴ Ibid., i.
- ²⁵ Ibid., vi.
- ²⁶ "Behind the Green Door" refers to the highly classified nature of certain IO capabilities.
- ²⁷ Air Force Doctrine Document (AFDD) 1. *Air Force Basic Doctrine* (17 November 2003): 6.
- ²⁸ Clancy, Tom; Horner, Chuck, General, USAF (ret); *Every Man a Tiger* (New York, NY, G. P. Putnam's Sons, 1999): 88.
- ²⁹ Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms* (12 April 2001): 208.
- ³⁰ The author represented ACC at the 2004 Air Force Doctrine Writing Committee (AFDD 2-5).
- ³¹ Air Force Doctrine Document (AFDD) 2-4. *Combat Support* (22 November 1999): 3.
- ³² *The Art of Command, enabled by the Science of Control* is a concept the author learned from General Hal Hornburg, former Commander of Air Combat Command.
- ³³ As of this writing, the Air Force Doctrine Center is planning to move ISR from AFDD 2.5.2 to AFDD 2-9. The author recommends reconsidering this decision in favor of an integrated AFDD 2-8 C2ISR containing two main sections: 1) AFFOR and Operational-Level C2, and 2) C2 Battle Management and ISR - Connecting the Operational and Tactical Levels of War.
- ³⁴ Force Doctrine Document (AFDD) 2-5. *Information Operations* (11 January 2005): Summary of Changes.
- ³⁵ Air Force Doctrine Document (AFDD) 2-5. *Information Operations* (4 January 2002): 18.
- ³⁶ Air Force Doctrine Document (AFDD) 2. *Organization and Employment of Aerospace Power* (17 February 2000): 54.
- ³⁷ Sun Tzu. *The Art of War*. Edited by James Clavell (New York, NY: Dell Publishing Co., Inc. September 1988): 11.
- ³⁸ Air Force Doctrine Document (AFDD) 1. *Air Force Basic Doctrine* (17 November 2003): 75.
- ³⁹ Joint Publication (JP) 3-0. *Doctrine for Joint Operations* (10 September 2001): III-9, A-1, V-1.
- ⁴⁰ Air Force Doctrine Document (AFDD) 2-5. *Information Operations* (11 January 2005): 1.
- ⁴¹ Ibid.
- ⁴² Air Force Doctrine Document (AFDD) 2-1. *Air Warfare* (22 January 2000): 9.
- ⁴³ Air Force Doctrine Document (AFDD) 2-5. *Information Operations* (11 January 2005): 5.
- ⁴⁴ D-I-M-E refers to the Diplomacy, Informational, Military, and Economic instrument of power.
- ⁴⁵ Air Force Doctrine Document (AFDD) 2-5. *Information Operations* (4 January 2002): 1.
- ⁴⁶ *Four-star Air Force conferences* refers to CORONA, Doctrine Summit, and Combat and Mobility Air Forces (CAF/MAF). The author prepared briefings and read-ahead materials for COMACC (including ACC's IO briefings at CORONA South and CORONA Fall 2003).
- ⁴⁷ IO is a specialized studies course and research seminar at Air Command and Staff College, and one of two required elective courses in the Air War College correspondence program.